"Express Mail" mailing label number EV 327 137 147 US
Date of Deposit 10/16/03

Our File No. 9281-4674
Client Reference No. FC US02033

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)
	)
Takehito Sugawara	)
	)
Serial No. To Be Assigned	)
	)
Filing Date: Herewith	)
	)
For: Handling Device and Method of Security Data	)
	)

SUBMISSION OF CERTIFIED COPY OF PRIORITY DOCUMENT

Mail Stop Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Transmitted herewith is a certified copy of priority document Japanese Patent Application No. 2002-301948 filed on October 16, 2002 for the above-named U.S. application.

Respectfully submitted,

Gustavo Siller, Jr.
Registration No. 32,305
Attorney for Applicant
Customer Number 00757

BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, ILLINOIS 60610
(312) 321-4200

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００２年１０月１６日

出 願 番 号
Application Number: 特願２００２－３０１９４８

[ST. 10/C]: [ＪＰ２００２－３０１９４８]

出 願 人
Applicant(s): アルプス電気株式会社

２００３年 ８月１４日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３０６５８４０

【書類名】　特許願
【整理番号】　A7021
【提出日】　平成14年10月16日
【あて先】　特許庁長官殿
【国際特許分類】　E05B 49/00
【発明の名称】　セキュリティ関連データの取り扱い装置及びその取り扱い方法
【請求項の数】　5
【発明者】
【住所又は居所】　東京都大田区雪谷大塚町１番７号　アルプス電気株式会社内
【氏名】　菅原　健人
【特許出願人】
【識別番号】　000010098
【氏名又は名称】　アルプス電気株式会社
【代理人】
【識別番号】　100078134
【弁理士】
【氏名又は名称】　武　顕次郎
【電話番号】　03-3591-8550
【選任した代理人】
【識別番号】　100093492
【弁理士】
【氏名又は名称】　鈴木　市郎
【選任した代理人】
【識別番号】　100087354
【弁理士】
【氏名又は名称】　市村　裕宏

【選任した代理人】

【識別番号】　100099520

【弁理士】

【氏名又は名称】　小林　一夫

【手数料の表示】

【予納台帳番号】　006770

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0010414

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　セキュリティ関連データの取り扱い装置及びその取り扱い方法

【特許請求の範囲】

【請求項１】　携帯器認証部、不揮発性メモリ、制御部を有する車載器と、前記車載器、車載装置、通信部を有する車両と、前記通信部と通信して前記車両の車載装置の制御を指示する携帯器と、を備え、

前記車両のセキュリティに関連するデータを暗号キーを用いて暗号化する暗号化部を前記車載器の制御部と不揮発性メモリの間に介在させ、

前記制御部からの指示で前記セキュリティ関連データを前記暗号キーを用いて暗号化して前記不揮発性メモリに格納する

ことを特徴とするセキュリティ関連データの取り扱い装置。

【請求項２】　請求項１において、

前記暗号キーは、前記セキュリティ関連データの暗号化信号を格納する前記不揮発性メモリとは別の不揮発性性メモリに格納されることを特徴とするセキュリティ関連データの取り扱い装置。

【請求項３】　請求項２において、

前記セキュリティ関連データは携帯器ＩＤを含み、前記不揮発性メモリはＥＥＰＲＯＭであり、前記別の不揮発性メモリはＲＯＭであることを特徴とするセキュリティ関連データの取り扱い装置。

【請求項４】　請求項３において、

前記ＥＥＰＲＯＭには前記携帯器ＩＤに加えて車載器ＩＤを格納することを特徴とするセキュリティ関連データの取り扱い装置。

【請求項５】　携帯器認証部、不揮発性メモリ、制御部を有する車載器と、前記車載器、ドアロック機構、通信部を有する車両と、前記通信部と通信して前記車両のドアロック機構をロック又はアンロックさせる携帯器と、を備えて、前記車両のセキュリティに関連するデータの取り扱い方法であって、

前記車載器の制御部と不揮発性メモリの間に設けられた暗号化部で前記セキュリティ関連データを暗号キーを用いて暗号化し、

前記暗号化した暗号化信号を前記不揮発性メモリに格納するとともに、前記暗

号キーを前記不揮発性メモリとは別の不揮発性性メモリに格納する

ことを特徴とするセキュリティ関連データの取り扱い方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、携帯器との通信によって車両ドアのロック、アンロックを自動的に実行する際、リモートキーレスエントリ（ＲＫＥ）におけるＩＤコード及び暗号キー等のセキュリティ関連データを取り扱う技術に関する。

【０００２】

【従来の技術】

図３に、リモートキーレスエントリ（ＲＫＥ）のブロック構成とＩＤコード及び暗号キー等のセキュリティ関連データの取り扱い方法を示す。図３において、車両１は、ドアロック機構５を有してそのドアの開閉を検出する検出部４を備えている。更に、車両１内には車載器２が設置され、車載器２は、携帯器２０からのドアロック、アンロックの信号を携帯器送受信アンテナ３を通して携帯器認証部６で携帯器ＩＤを認証し、認証の結果、ＩＤ合格ならばドアをロック、アンロックするように統括制御部７でドアロック機構を制御する。その際、ＥＥＰＲＯＭ９にはＩＤ（車両ＩＤ、携帯器ＩＤ）及び暗号キー（携帯器と車両とは暗号キーによって暗号化された信号で通信する）を記憶し、ＲＯＭ８には統括制御のためのプログラムを記憶する。

【０００３】

従来、車両のドアロック機構をロックしたりアンロックするリモートキーレスエントリ（ＲＫＥ）には、携帯器から車載器への一方向通信であるマニュアルＲＫＥの他に、携帯器と車載器とで双方向通信を行うパッシブ（Ｐａｓｓｉｖｅ）ＲＫＥが知られている。このパッシブＲＫＥは、車両、例えば自動車のドアロックのロック、アンロックを自動的に行うもので、人間の携帯する携帯器と車両に搭載される車載器との間で双方向の通信を行い、携帯器ＩＤや車両ＩＤの認証の結果、正当な携帯器であることを車載器が確認したときにドアロック機構５に対してロック又はアンロックの動作を行う。この際、認証のために、携帯器及び車

載器は互いの認証を行うためにユニークなＩＤ（Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ Ｃｏｄｅ；認証コード）と暗号キー（Ｋｅｙ）を有し、それぞれの通信時には、ＩＤを含むデータを暗号キーで暗号化した信号で通信する。

【０００４】

パッシブＲＫＥの具体的機能を説明すると、車載器２は一定周期毎にリクエスト信号を発信する。リクエスト信号には車載器ＩＤが含まれ、比較的短い距離にしか到達しない。携帯器２０がリクエスト信号の到達範囲外にあるときは携帯器はこのリクエスト信号を受信することはない。一方、携帯器を携帯する人間が自動車に接近し、リクエスト信号の到達範囲に至ると携帯器はリクエスト信号を受信し、リクエスト信号中の車載器ＩＤをチェックし、それが正当な車載器から発せられたものであると認識すると、携帯器はレスポンス信号を発信する。

【０００５】

車載器はレスポンス信号を受信し、その中に含まれる携帯器ＩＤを取り出し、メモリに登録されている携帯器ＩＤと前記レスポンス信号中の携帯器ＩＤを照合し、一致したときは、ドアロック機構５に対して、アンロック信号を発信し、ドアロックをアンロック（解除）させる。照合が不成功に終わると、ロック機構に対して制御信号を発信しない。また、携帯器を持った人間が、車両から降りて離れるときには、携帯器がリクエスト信号を受信できなくなった時点で、つまり車載器がレスポンス信号を受信できなくなった時点で、車載器はドアロック機構に対してロック信号を発信する。

【０００６】

リクエスト信号とレスポンス信号は、携帯器と車載器が共通に記憶している暗号化キーによって暗号化されて発信され、受信した側は、自己が記憶している暗号キーで信号を解読する。

【０００７】

ＩＤ、暗号化キー等のセキュリティ関連データは、バッテリを外されても記憶していなければならないため、ＥＥＰＲＯＭやＲＯＭなどの不揮発性メモリへ格納している。ＥＥＰＲＯＭやＲＯＭへ格納しているデータは固有データそのままの形式の情報値である。特に、車載器においては、携帯器ＩＤが次に示すような

特殊事情のために、ＲＯＭではなくて、ＥＥＰＲＯＭに記憶される。そして、特殊事情とは、車載器においては最初から携帯器ＩＤが記憶されているわけではなく、任意の携帯器（１台の車両に対してＩＤの異なる複数の携帯器）からのレスポンス信号を受けた車載器が、信号を分析し、その携帯器に予め記憶された携帯器ＩＤを取り出して自己の不揮発性メモリに記憶することである。

【０００８】

そして、この作業は、自動車ディーラやユーザが随時に行うことができるので、携帯器と車載器を製造工場でペアリング（対応付け）しなくても済むというメリットがある。しかし、上述したように後になってＩＤ登録するので、記憶媒体としてＲＯＭを用いることができない。更に、暗号キーも同様に、後になって、車載器と携帯器のいずれか一方から他方に送信された信号を介して他方に登録されるために（図３では携帯器にメモリが図示されていないが、携帯器にメモリがある）、ＲＯＭではなくＥＥＰＲＯＭに記憶されている。

【０００９】

【発明が解決しようとする課題】

上述した従来技術において、不揮発性メモリとしてのＲＯＭは、ＲＯＭ内の記憶内容の解読を阻止する構造を採用しているので、解読するにしても多くの時間と手間を必要とする。これに対して、通常、ＥＥＰＲＯＭはその構造上ＩＣの仕様にしたがえば記憶内容の解析が比較的容易である。したがって、ＥＥＰＲＯＭに記憶された携帯器ＩＤや暗号キーのデータが他人に解読され、その規則性などが分析されてしまうと、多数の自動車のセキュリティが崩壊してしまうという事態に発展する虞が生じる。従来技術では、ＩＤ、暗号化キー等のセキュリティ関連データがそのままの値をＥＥＰＲＯＭに格納して、自動車のセキュリティの観点で課題が生じていた。

【００１０】

本発明の目的は、不揮発性メモリであるＥＥＰＲＯＭ及び／又はＲＯＭに格納しなければならないセキュリティ関連データを暗号化して格納することで、データを仮に読み取られても解読できないようにすることにある。

【００１１】

【課題を解決するための手段】

前記課題を解決するために、本発明は次のような構成を採用する。

携帯器認証部、不揮発性メモリ、制御部を有する車載器と、前記車載器、車載装置、通信部を有する車両と、前記通信部と通信して前記車両の車載装置の制御を指示する携帯器と、を備え、前記車両のセキュリティに関連するデータを暗号キーを用いて暗号化する暗号化部を前記車載器の制御部と不揮発性メモリの間に介在させ、前記制御部からの指示で前記セキュリティ関連データを前記暗号キーを用いて暗号化して前記不揮発性メモリに格納するセキュリティ関連データの取り扱い装置。また、携帯器認証部、不揮発性メモリ、制御部を有する車載器と、前記車載器、ドアロック機構、通信部を有する車両と、前記通信部と通信して前記車両のドアロック機構をロック又はアンロックさせる携帯器と、を備えて、前記車両のセキュリティに関連するデータの取り扱い方法であって、前記車載器の制御部と不揮発性メモリの間に設けられた暗号化部で前記セキュリティ関連データを暗号キーを用いて暗号化し、前記暗号化した暗号化信号を前記不揮発性メモリに格納するとともに、前記暗号キーを前記不揮発性メモリとは別の不揮発性性メモリに格納するセキュリティ関連データの取り扱い方法。このようなセキュリティ関連データの取り扱い装置又は方法によって、セキュリティ関連データを不揮発性メモリに保管するに際して暗号キーを用いて暗号化した信号形式で格納するので、車両のセキュリティ関連データを解読される虞は無くなる。

【００１２】

また、前記セキュリティ関連データの取り扱い装置において、前記暗号キーは、前記セキュリティ関連データの暗号化信号を格納する前記不揮発性メモリとは別の不揮発性性メモリに格納される構成とした。更に、前記セキュリティ関連データの取り扱い装置において、前記セキュリティ関連データは携帯器ＩＤを含み、前記不揮発性メモリはＥＥＰＲＯＭであり、前記別の不揮発性メモリはＲＯＭである構成とした。これらの構成によって、携帯器ＩＤなどのセキュリティ関連データの取り扱いに際して、暗号キーは解読され難いＲＯＭなどの不揮発性メモリに記憶保管しておくので暗号キーが読み出される虞は無くなる。

【００１３】

【発明の実施の形態】

本発明の実施形態に関するセキュリティ関連データの取り扱い装置及び方法について、図１と図２を参照しながら説明する。図１は、本発明の実施形態に係る、リモートキーレスエントリにおけるＩＤコード及び暗号キー等のセキュリティ関連データの取り扱いシステムを示すブロック図であり、図２は、本実施形態に関する、セキュリティ関連データのＥＥＰＲＯＭへの格納フローを示す図である。

【００１４】

図面において、１は車両、２は車載器、３は携帯器送受信アンテナ、４はドア開閉検出部、５はドアロック機構（車載装置）、６は携帯器認証部、７は統括制御部、８はＲＯＭ、９はＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ　Ｅｒａｓａｂｌｅ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｒｅａｄ－Ｏｎｌｙ　Ｍｅｍｏｒｙ）、１０はデータ暗号化制御部、２０は携帯器、２１は携帯器アンテナ、２２は携帯器内ＥＥＰＲＯＭ、をそれぞれ表す。

【００１５】

図１において、車両１と携帯器２０とはパッシブキーレスエントリを構成しており、車載器２と携帯器２０とで双方向通信を行ってドアロックのロック又はアンロックを自動実行するとともに車両の保安管理を厳重にしたキーレスエントリである。即ち、携帯器２０が車載器２からのリクエスト信号の到達領域に入ると、携帯器２０はリクエスト信号を受信することでレスポンス信号を発信し、車載器２はレスポンス信号を受信してＩＤ照合の結果、ドアロックを解除（アンロック）するようになっている。更に、携帯器２０が車両１から離れるときは、車載器２０が携帯器２０からのレスポンス信号を受信できなくなったときにドアロック機構５に対してドアロックするように動作するものである。

【００１６】

具体的に説明すると、車載器２から車載器ＩＤを含んだリクエスト信号をアンテナ３を通して一定周期毎に携帯器２０に送信し、一方、携帯器２０からはアンテナ２１を通して携帯器ＩＤを含んだレスポンス信号を車載器２に送信して、双方向通信を行う。車載器２の携帯器認証部６において、携帯器２０からのレスポ

ンス信号に含まれた携帯器ＩＤと、予めＥＥＰＲＯＭ９に記憶されていた携帯器ＩＤとを照合し、ＩＤ照合が一致したときは、統括制御部７はドアロック機構５にアンロック信号を発してドアロックを解除する。ＩＤ照合が一致しないときは統括制御部７はドアロック機構５にアンロック信号を発せず、ドアロックを解除しない。

【００１７】

ここで、車載器２からのリクエスト信号及び携帯器２０からのレスポンス信号は、携帯器と車載器が共に記憶している第１の暗号キーによって共に暗号化されて発信され、受信側では自己が記憶している第１の暗号キーでリクエスト信号又はレスポンス信号を解読するようになっている。

【００１８】

また、リモートキーレスエントリ（ＲＫＥ）を使用するに当たって、レスポンス信号に含まれる携帯器ＩＤは、車載器をＩＤ登録モードに設定した後携帯器２０から発せられたレスポンス信号を車載器で分析して各携帯器独自の携帯器ＩＤを取り出してＥＥＰＲＯＭ９に記憶することにより新規に車載器に登録される。換言すると、車載器２には当初から予め規定された携帯器ＩＤが記憶されている訳ではなく、携帯器の携帯器ＩＤを学習して記憶している。このように、携帯器ＩＤを車載器製造完了と同時ではなくて、ＲＫＥの使用開始前に記憶する必要があるために、携帯器ＩＤは、不揮発性メモリの内でＲＯＭでなく、ＥＥＰＲＯＭに記憶する。

【００１９】

図１における車両１のＥＥＰＲＯＭ９には、上述したように、当該車両に対する複数の携帯器に付された携帯器ＩＤの他に、当該車両の車載器ＩＤを格納している。ここで、複数の携帯器に対して、それぞれ異なるＩＤを付しても良いし、同一のＩＤを付しても良く、更に、グループ別に異なるＩＤを付しても良い。

【００２０】

また、ＥＥＰＲＯＭ９に記憶されるＩＤ（携帯器ＩＤ、車載器ＩＤ）は、データ暗号化制御部１０によって第２の暗号キーによって暗号化された信号であり、これが、本発明の特徴の一つである。従来技術のようにＩＤをそのままの信号形

式でＥＥＰＲＯＭに記憶すれば、ＥＥＰＲＯＭの構造上解読される虞があり、車両のセキュリティの観点で不安が生じる。本発明では、第２の暗号キーを用いてＩＤを暗号化してＥＥＰＲＯＭ９に記憶しているので、例え、そのデータを読み取られても解読はできないものである。そして、この第２の暗号キーは、リクエスト信号及びレスポンス信号に対する第１の暗号キーと共に、解読ができ難いＲＯＭ８に格納される。

【００２１】

また、図２には、携帯器からのレスポンス信号に含まれる携帯器ＩＤを取り出してＥＥＰＲＯＭに記憶するフローを示している。統括制御部７からＥＥＰＲＯＭへデータ（例えば、携帯器ＩＤ）を格納する指示が発生すると（ステップ１）、データ暗号化制御部１０は、或る関数ｆ２（Ｅ－Ｋｅｙ，ｄａｔａ）＝Ｅ－ｄａｔａを用いることによってセキュリティ関連データを暗号化させる（ステップ２）。ここで、ｆ２（ｘ，ｙ）は第２の暗号キーを用いた暗号化関数であり、Ｅ－ＫｅｙはＥＥＰＲＯＭへ格納するデータを暗号化させる暗号キーであり、ｄａｔａはＥＥＰＲＯＭへ格納するセキュリティ関連データであり、Ｅ－ｄａｔａはＥＥＰＲＯＭ格納用にｄａｔａを暗号化したものである。また、或る関数ｆ２－１（Ｅ－Ｋｅｙ，Ｅ－ｄａｔａ）＝ｄａｔａを用いて暗号化データ復元させる。次に、ステップ３で暗号化データをＥＥＰＲＯＭに格納する。

【００２２】

以上説明したように、本発明によれば、車載器と携帯器との通信に使用するデータ（例えば、リクエスト信号、レスポンス信号）を第１の暗号キーによって暗号化するとともに、ＲＯＭではなくてＥＥＰＲＯＭに格納すべきセキュリティ関連データ（例えば、ＩＤ）を第２の暗号キーによって暗号化して、解読をできなくさせるものであり、その際、第１の暗号キーと第２の暗号キーはともに解読でき難いＲＯＭに格納しておく。

【００２３】

車載器のＥＥＰＲＯＭ９に携帯器ＩＤを格納することを例示して説明したが、このＥＥＰＲＯＭ９には携帯器ＩＤに加えて、車載器ＩＤも格納されていて、この車載器ＩＤも同様に第２の暗号キーで暗号化されている。また、携帯器２０に

もＥＥＰＲＯＭ２２や不図示の制御部を設けて、この不揮発性メモリに車載器ＩＤや当該携帯器ＩＤを暗号化して格納しても良い。

【００２４】

また、一定周期毎にリクエスト信号を発信するパッシブＲＫＥを例示して説明したが、トリガスイッチを例えばドアハンドルに設け、トリガスイッチを操作したときにリクエスト信号の発信が開始されるようにしても良い。更に、車載装置がドアロック機構であることを例示して説明したが、車載装置はこれに限定されず、例えばエンジン始動装置など他の装置であっても良い。エンジン始動装置の場合、トリガスイッチはメカニカルキーを挿入するイグニッションシリンダに内蔵されたり、又は単独のスイッチとしても良い。

【００２５】

【発明の効果】

本発明によれば、セキュリティ関連データを不揮発性メモリに保管するに際して暗号キーを用いて暗号化した信号形式で格納するので、車両のセキュリティ関連データを解読される虞は無くなる。

【００２６】

また、暗号キーは解読され難いＲＯＭ等の不揮発性メモリに記憶保管しておくので暗号キーが読み出される虞は無くなる。

【００２７】

更に、リモートキーレスエントリにおけるリクエスト信号やレスポンス信号における通信に際しても他の暗号キーで暗号化して双方向通信することでセキュリティを確保すると共に、当該他の暗号キーも解読され難いＲＯＭ等の不揮発性メモリに記憶保管しておくので当該他の暗号キーも読み出される虞は無くなる。

【図面の簡単な説明】

【図１】

本発明の実施形態に係る、リモートキーレスエントリにおけるＩＤコード及び暗号キー等のセキュリティ関連データの取り扱いシステムを示すブロック図である。

【図２】

本実施形態に関する、セキュリティ関連データのＥＥＰＲＯＭへの格納フローを示す図である。

【図３】

従来技術に関する、リモートキーレスエントリのブロック構成とＩＤコード及び暗号キー等のセキュリティ関連データの取り扱い方法を示す図である。

【符号の説明】

１　車両

２　車載器

３　携帯器送受信アンテナ

４　ドア開閉検出部

５　ドアロック機構（車載装置）

６　携帯器認証部

７　統括制御部

８　ＲＯＭ

９　ＥＥＰＲＯＭ

１０　データ暗号化制御部

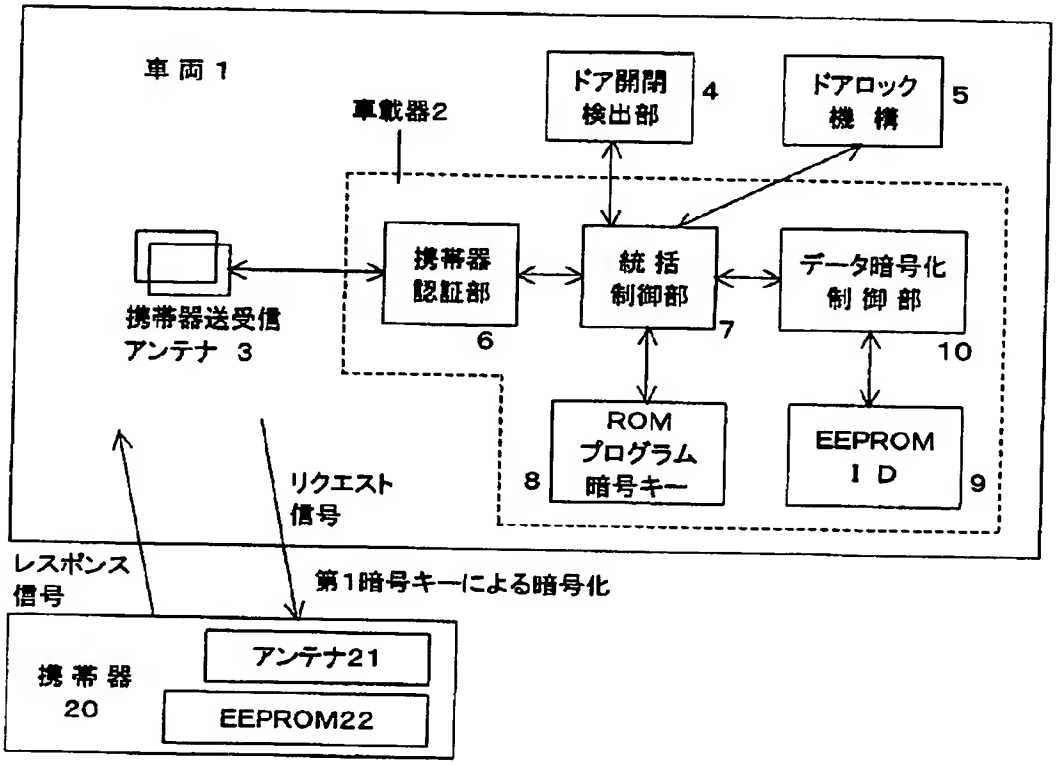
２０　携帯器

２１　携帯器アンテナ

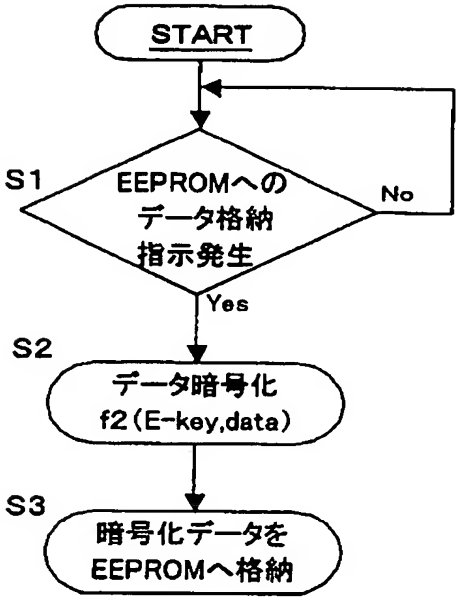
２２　ＥＥＰＲＯＭ

【書類名】　図面

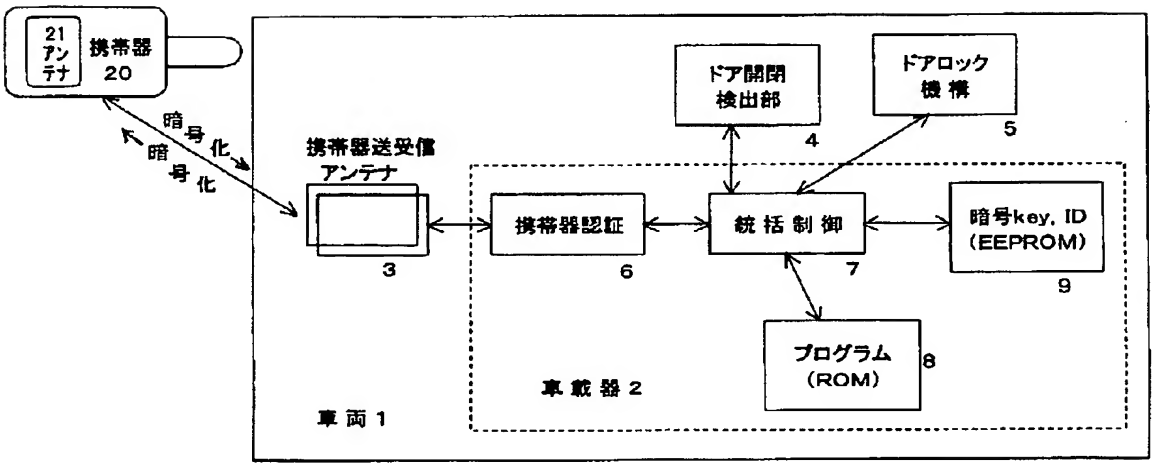
【図１】


車両１
車載器2
ドア開閉
検出部
4
ドアロック
機構
5
携帯器
認証部
6
統括
制御部
7
データ暗号化
制御部
10
携帯器送受信
アンテナ 3
ROM
プログラム
暗号キー
8
EEPROM
ＩＤ
9
リクエスト
信号
レスポンス
信号
第1暗号キーによる暗号化
携帯器
20
アンテナ21
EEPROM22

【図２】


START
S1
EEPROMへの
データ格納
指示発生
No
Yes
S2
データ暗号化
f2(E-key,data)
S3
暗号化データを
EEPROMへ格納

【図３】


21
アンテナ
携帯器
20
暗号化
暗号化
携帯器送受信
アンテナ
3
ドア開閉
検出部
4
ドアロック
機構
5
携帯器認証
6
統括制御
7
暗号key, ID
(EEPROM)
9
プログラム
(ROM)
8
車載器２
車両１

【書類名】　　要約書

【要約】

【課題】　不揮発性メモリに格納しなければならないセキュリティ関連データ（例えば、携帯器ＩＤ）を暗号化して格納することで、データを仮に読み取られても解読できないようにすること。

【解決手段】　携帯器認証部６、ＥＥＰＲＯＭ９、ＲＯＭ８、制御部７を有する車載器２と、車載器２、ドアロック機構５、通信部３を有する車両１と、車両１のドアロック機構５をロック又はアンロックさせる携帯器２０と、を備えて、車両のセキュリティに関連するデータ（例えば、携帯器ＩＤ）を取り扱う装置において、セキュリティ関連データを暗号キーを用いて暗号化する暗号化部１０を制御部とＥＥＰＲＯＭの間に介在させ、携帯器認証部の認証結果に基づいて制御部からの指示で携帯器ＩＤを暗号キーを用いて暗号化してＥＥＰＲＯＭ９に格納するとともに、暗号キーはＲＯＭ８に格納すること。

【選択図】　　図１

特願２００２－３０１９４８

出　願　人　履　歴　情　報

識別番号　　［０００００１００９８］

１．変更年月日　　１９９０年　８月２７日
［変更理由］　　新規登録
住　所　　東京都大田区雪谷大塚町１番７号
氏　名　　アルプス電気株式会社